UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,413	10/16/2003	Robert E. Cavanaugh	58895/P004US/10306553	8593

29053 7590 12/13/2007

FULBRIGHT & JAWORSKI L.L.P
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
12/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/687,413	CAVANAUGH, ROBERT E.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 11-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 11-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/24/07 and 5/25/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Wexler et al. U.S. Pub. No. 20030229809 (hereinafter Wexler).

4. As per claim 1, Wexler discloses a security system for use in conjunction with data flowing from a first device to a second device being directed to said second device in accordance with a network address of said second device, said system comprising: a security device connected between said first and second devices (Wexler: [0009]: proxy server), said security device accepting packet data for bridging to said second device (Wexler: [0009]: handles packets), said security device operable for observing data flowing from said first device to said second device, said security device not itself having a network address (Wexler: [0010]-[0011]: the proxy server does not have an IP address... proxy server changes contents of some of the packets it forwards), and configured to be inserted between said first and said second device

while a network connection is active (Wexler: [0009] lines 10-12: the transparent proxy server eliminates the need to configure network elements).

5. As per claim 2, Wexler discloses the system of claim 1. Wexler further discloses wherein said first device could be any device on the unsecured side of said security device, each said first device having a unique network address (Wexler: [0038]: source IP address), and wherein said second device could be any device on the secured side of said security device (Wexler: [0047] and figure 1: proxy protects local area network), each said second device having a unique network address (Wexler: [0038]: destination IP address).

6. As per claim 3, Wexler discloses the system of claim 2. Wexler further discloses wherein said security device maintains a list of addresses for which it has security responsibility and wherein said security device only observes those data packets containing the network addresses maintained in said list (Wexler: [0056]).

7. As per claim 4, Wexler discloses the system of claim 3. Wexler further discloses wherein said list includes addresses of both said first devices and said second devices (Wexler: [0056]: store IP addresses for security verification; [0062]: manages a list of expected packets; [0072]-[0073]: the tables include source and destination IP addresses).

8. As per claim 5, Wexler discloses the system of claim 1. Wexler further discloses wherein said observing comprises: a monitoring system for gathering information pertaining to the

operation of said second device (Wexler: [0072]: inbound and outbound reception table and transmission table); and a mechanism for modifying the flow of data into said security system depending upon said gathered information (Wexler: [0023]: modifying some fields of the packets).

9. As per claim 6, Wexler discloses the system of claim 5. Wexler further discloses wherein said gathered information is selected from the list containing: number of arriving packets in a particular time interval; the type of requests contained within given packets; the nature of the informational content of the packets; the sending identity of the packets; the destination of the packets; the traffic patterns formed by packets from specific sources; the number of arriving packets from specific sources; the correctness of the packets; certain data contained in one or more messages; and the type of file attached to a message (Wexler: [0072]-[0073]: storing information pertaining to operation of the proxy server; [0060]: functions of the proxy server).

10. As per claim 7, Wexler discloses the system of claim 5. Wexler further discloses wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits (Wexler: [0072]-[0073]: the tables are created for allowing communication between source and destination; [0104]: the table entry is erased upon time-out), and wherein said operational characteristics of said mechanism is modified in accordance with said set limits (Wexler: [0104]: when the entry is erased, session is closed).

11. As per claim 8, Wexler discloses a security device for use in a packet data network where packets are delivered from a sending location to a destination location based upon one or more destination network addresses associated with each packet (Wexler: [0009]: proxy server), said security device comprising: at least one NIC card for receiving data packets (Wexler: [0047]: inbound and outbound ports); a database for maintaining a list of destination network addresses to be secured by said device (Wexler: [0056]: proxy is configured with IP addresses of the entities in the local network); wherein said at least one NIC card is connected to said network at any point between a sending location and one or more destination locations (Wexler: [0047]: the inbound and outbound ports are connected to external router for Internet and edge router for local network), said NIC card maintained in promiscuous mode such that said security device can observe all data directed to any destination addresses maintained from time to time in said list (Wexler: [0056]: the proxy server operates in Promiscuous mode); wherein said security device is connected to said network without establishing a network address for said security device (Wexler: [0009]: the proxy server is intercepts packets that is not directed to the proxy server; [0010]: the proxy server does not have an IP address); and wherein said security device can be moved from location to location on said network without changing any network settings (Wexler: [0009]: the transparent proxy server eliminates the need to configure network elements with the identity of the proxy server).

12. As per claim 11, Wexler discloses the device of claim 8. Wexler further discloses the method comprises a plurality of NIC cards all operating in said promiscuous mode (Wexler: [0056]: all packets are processed under Promiscuous mode).

13. As per claim 12, Wexler discloses the device of claim 11. Wexler further discloses wherein said security device has a zero network footprint while said NIC cards are in said promiscuous mode (Wexler: [0048]: the edge router and external router are not aware in layer 2 and layer 3 of the presence of proxy server).

14. As per claim 13, Wexler discloses the device of claim 12. Wexler further discloses wherein all of said NIC cards share the same destination list (Wexler: [0047]: inbound and outbound ports can transmit and receive data; [0068]: incoming and outgoing packets are verified according to destination IP address).

15. As per claim 14, Wexler discloses the device of claim 8. Wexler further discloses wherein said observing comprises: monitoring system for gathering information pertaining to the operation of said second device (Wexler: [0072]: inbound and outbound reception table and transmission table); and mechanism for modifying the flow of data into said security system depending upon said gathered information (Wexler: [0023]: modifying some fields of the packets).

16. As per claim 15, Wexler discloses the device of claim 14. Wexler further discloses wherein said gathered information is selected from the list containing: number of arriving packets in a particular time interval; the type of requests contained within given packets; the nature of the informational content of the packets; the sending identity of the packets; the

destination of the packets; the traffic patterns formed by packets from specific sources; the number of arriving packets from specific sources; the correctness of the packets; certain data contained in one or more messages; and the type of file attached to a message (Wexler: [0072]-[0073]: storing information pertaining to operation of the proxy server; [0060]: functions of the proxy server).

17. As per claim 16, Wexler discloses the device of claim 15. Wexler further discloses wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits (Wexler: [0072]-[0073]: the tables are created for allowing communication between source and destination; [0104]: the table entry is erased upon time-out), and wherein said operational characteristics of said mechanism is modified in accordance with said set limits (Wexler: [0104]: when the entry is erased, session is closed).

18. As per claim 17, Wexler discloses a method for monitoring data packets arriving at a destination device, said data packets including a network address said packets traveling on a network defined in accordance with said network addresses (Wexler: [0009]: proxy server intercepts packets directed to destination IP addresses), said method comprising the steps of: inserting a security device into said network at a particular location between a sending device and a destination device (Wexler: [0047]: the proxy server is located between source and destination device); and establishing within said security device the network addresses of said destination device (Wexler: [0056]: proxy server is configured with IP addresses of the entities of local network).

19. As per claim 18, Wexler discloses the method of claim 17. Wexler further discloses wherein said destination device is a plurality of devices and wherein said establishing step comprises: establishing all of said plurality of destination devices within said security device (Wexler: [0056]: configure IP addresses of entities of local network).

20. As per claim 19, Wexler discloses the method of claim 18. Wexler further discloses wherein at least one of said destination devices is on a public side of said security device so as to monitor data packets egressing from a private side of security device (Wexler: [0068]: monitor packets received from inbound port toward outbound is monitored).

21. As per claim 20, Wexler discloses the method of claim 17. Wexler further discloses the step of: setting said security device to operate in the promiscuous mode (Wexler: [0056]: proxy server operates in Promiscuous mode).

22. As per claim 21, Wexler discloses the method of claim 20. Wexler further discloses the step of: modifying the delivery of data to said destination based upon the content of information in arriving data packets (Wexler: [0060]: well known functions of proxy server).

23. As per claim 22, Wexler discloses the method of claim 17. Wexler further discloses wherein said security device does not have a network location address (Wexler: [0010]: proxy

server does not have IP address; [0048]: the external and internal network is not aware of the proxy server in layer 2 and layer 3).

24. As per claim 23, Wexler discloses the method of claim 22. Wexler further discloses the steps of: blocking certain data packets from reaching said destination device (Wexler: [0060]: proxy server functions; blocking all packets from reaching said destination device (Wexler: [0060]: redirection) ; load balancing between devices (Wexler: [0060]: load balancing); modifying the informational content of certain ones of said packets (Wexler: [0060]: correctness check...change portions of the packets); unblocking certain hitherto blocked packets, on the basis of certain parameters (Wexler: [0060]: access control); and modifying the informational content of certain ones of said packets (Wexler: [0060]: change content).

25. As per claim 24, Wexler discloses the method of claim 17. Wexler further discloses the steps of: monitoring data packets leaving said destination device (Wexler: [0068]: bi-directional monitoring); and selectively modifying the operational characteristics of any network traveled by said data packets based upon the content of said leaving packets (Wexler: [0060]: proxy server functions...change portions of the packets).

26. As per claim 25, Wexler discloses the method of claim 17. Wexler further discloses wherein said inserting step can be accomplished without changing network configuration settings (Wexler: [0009]: the transparent proxy server eliminates the need to configure network elements with the identity of the proxy server).

27. As per claim 26, Wexler discloses the method of claim 17. Wexler further discloses wherein said inserting step can be performed while said network is operating (Wexler: [0009]: no need to change settings).

28. As per claim 27, Wexler discloses the method of claim 17. Wexler further discloses the step of: removing said security device form said particular location while said network is operating (Wexler: [0016]: the transparency module is located on the switch).

29. As per claim 28, Wexler discloses a security device for connection in a data network ahead of a plurality of data destinations to be protected, each said destination identifiable by a unique network address (Wexler: [0056]: protect entities in local network), said security device comprising: means for accepting data packets from said network without said data packets being addressed to said security device (Wexler: [0009]: intercepts packets directed to destination IP addresses); and means for passing accepted data packets to particular ones of said data destinations in accordance with destination addresses of said destinations to be detected and maintained for said security device (Wexler: [0048]: forwards packets to same IP addresses as they are received).

30. As per claim 29, Wexler discloses the device of claim 28. Wexler further discloses wherein said maintained destination addresses are stored in a database internal to said security device (Wexler: [0056]: store the IP addresses into the proxy server).

31. As per claim 30, Wexler discloses the device of claim 28. Wexler further discloses wherein said accepting means comprises: at least one network termination operating in a promiscuous mode (Wexler: [0056]).

32. As per claim 31, Wexler discloses a method of operating a security device connected to a data network ahead of a plurality of data destinations to be protected, each said destination identifiable by a unique network address (Wexler: [0056]: protect entities in local network), said data network having a plurality of nodes (Wexler: [0056]), said method comprising the steps of: accepting data packets from said network without said data packets being addressed to said security device (Wexler: [0009]: intercepts packets directed to destination IP addresses); and passing accepted data packets to particular ones of said data destinations in accordance with destination addresses of said destinations to be detected and maintained for said security device (Wexler: [0048]: forwards packets to same IP addresses as they are received).

33. As per claim 32, Wexler discloses the method of claim 31. Wexler further discloses the method comprises real time review of certain parameters pertaining to data flowing between nodes of said network (Wexler: [0056]: all packets are passed to processor of proxy server); means for comparing said monitored parameters against stored criteria (Wexler: [0060]: well known functions of proxy server); and means for feeding data traffic affecting signals to one or more of said nodes under at least partial control of said comparing means (Wexler: [0060]: changing portions of the packets including traffic redirection).

34. As per claim 33, Wexler discloses the method of claim 32. Wexler further discloses wherein said stored criteria are dynamically changeable (Wexler: [0104]: each entry has time-out field which is periodically decremented).

35. As per claim 34, Wexler discloses the method of claim 32. Wexler further discloses the method comprises the step of: storing certain of said monitored parameters for a period of time, at least some of said stored parameters being useful in determining at least a portion of the communication history of said monitored data (Wexler: [0079]: timestamp; [0103]: time-out field).

36. As per claim 35, Wexler discloses the method of claim 32. Wexler further discloses wherein at least one of said nodes to which data traffic attaches signals is a gateway node to said destination to be protected (Wexler: [0072]-[0073]: maintain tables to record IP addresses of inbound and outbound messages).

Response to Arguments

37. Applicant's arguments filed on 9/21/07 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the Wexler reference does not disclose wherein the security device is configured to be inserted between said first and said second device while a network connection is active. However, Wexler discloses the a transparent

proxy server that eliminates the need to configure network elements and it functions without configuration (Wexler: [0009]). One with ordinary skill in the art understands that configuration causes network to be temporarily deactivated and by providing a transparent proxy server that eliminates configuration need, network can continue to function without interruption. Therefore, applicant's argument is traversed.

Conclusion

38. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100